PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-298942
(43)Date of publication of application : 24.10.2000

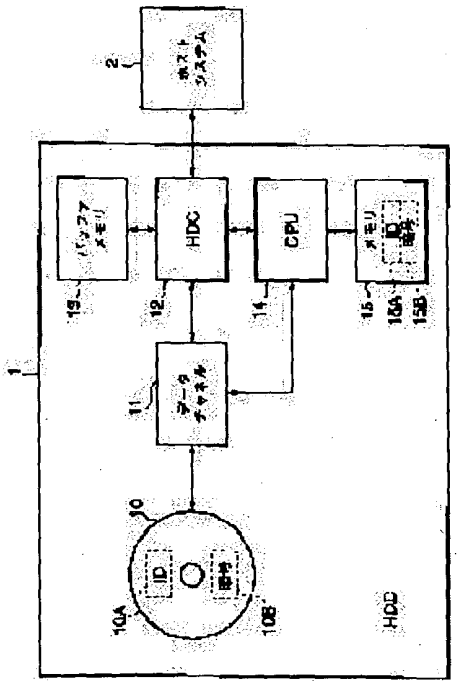
(51)Int.Cl. G11B 20/10
G06F 3/06
G06F 12/14
G11B 19/02
G11B 19/12

(21)Application number : 11-108173
(22)Date of filing : 15.04.1999

(71)Applicant : TOSHIBA CORP
(72)Inventor : KONISHI KAZUO
KATAGIRI TAKAHITO
AWAZU KOICHI

(54) DISK STORAGE DEVICE AND COPY PREVENTING SYSTEM APPLIED TO THIS DEVICE

(57)Abstract:
PROBLEM TO BE SOLVED: To obtain a disk storage device and a system using this device which have an effective copy preventing function to realize copyright protection of contents data as the result.
SOLUTION: With respect to an attachable/detachable small-ized HSS 1, ID data 10A peculiar to the device and encryption data 10B are stored in a redundant area (alternate sector) on a disk 10. A CPU 14 reads out ID data 10A and encryption data 10B from the disk 10 in accordance with a specific command from a host system 2 and transfers them. The host system 2 uses received data 10A and 10B to eneipher contents data and preserves it in the HDD 1.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－298942
（P2000－298942A）
(43)公開日　平成12年10月24日(2000.10.24)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｈ	５Ｂ０１７
			Ｆ	５Ｂ０６５
Ｇ０６Ｆ　3/06	３０４	Ｇ０６Ｆ　3/06	３０４Ｍ	５Ｄ０４４
			３０４Ｋ	５Ｄ０６６
12/14	３２０	12/14	３２０Ｅ	

審査請求　未請求　請求項の数９　ＯＬ　（全８頁）　最終頁に続く

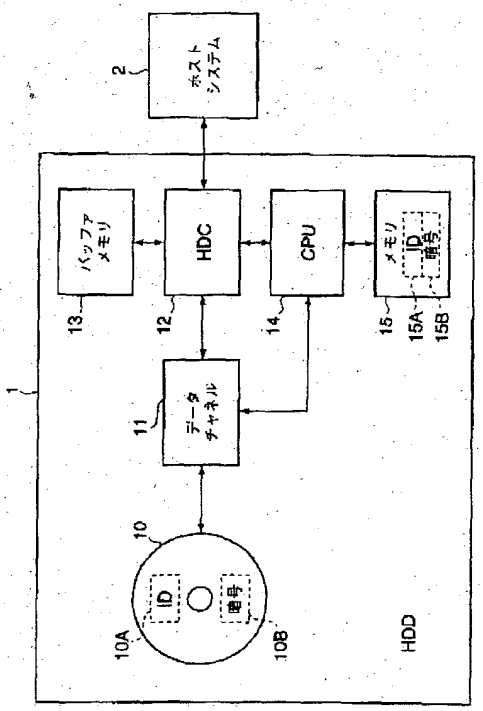
(21)出願番号　特願平11－108173
(22)出願日　平成11年４月15日(1999.4.15)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地
(72)発明者　小西　和夫
東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内
(72)発明者　片桐　孝人
東京都港区芝浦一丁目１番１号　株式会社東芝本社事務所内
(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　ディスク記憶装置及び同装置に適用するコピー防止システム

(57)【要約】
【課題】有効なコピー防止機能を有し、結果的にコンテンツデータの著作権保護を実現できるディスク記憶装置及び同装置を利用したシステムを提供することにある。
【解決手段】着脱可能な小型のＨＤＤ１において、ディスク１０上の冗長領域（代替セクタ）に装置固有のＩＤデータ１０Ａ及び暗号データ１０Ｂが記憶されている。ＣＰＵ１４は、ホストシステム２からの特定コマンドに応じて、ディスク１０からＩＤデータ１０Ａ及び暗号データ１０Ｂを読出して転送する。ホストシステム２は、受信した各データ１０Ａ，１０Ｂを利用して、コンテンツデータを暗号化してＨＤＤ１に保存する。



【特許請求の範囲】
【請求項１】　ユーザデータの記録領域、及び当該ユーザデータの記録動作では書換え不可能な記録領域であって固有の識別データが記録された特定の記録領域を有するディスク記憶媒体と、
ホストシステムからの特定コマンドに応じて、前記識別データを前記特定の記録領域から読出して前記ホストシステムに出力する制御手段とを具備したことを特徴とするディスク記憶装置。
【請求項２】　ディスク記憶媒体をデータの記録媒体として使用するディスク記憶装置であって、
装置固有の識別データを記憶し、前記ディスク記憶媒体とは区別されたメモリ手段と、
ホストシステムからの記録再生用のコマンドに応じて前記ディスク記憶媒体に対するデータの記録再生を制御し、当該ホストシステムからの特定コマンドに応じて前記メモリ手段から前記識別データを読出して前記ホストシステムに出力する制御手段とを具備したことを特徴とするディスク記憶装置。
【請求項３】　ディスク記憶媒体をデータの記録媒体として使用するディスク記憶装置に適用するコピー防止システムであって、
前記ディスク記憶媒体または前記ディスク記憶媒体とは区別されたメモリ手段に記憶された装置固有の識別データの読出し動作を制御する制御手段と、
前記制御手段を介して読出した前記識別データを使用して、前記ディスク記憶媒体に記録するコンテンツデータを暗号化するための暗号化キーデータを生成する暗号データ生成手段とを具備したことを特徴とするコピー防止システム。
【請求項４】　前記暗号化キーデータを使用して、指定のコンテンツデータを暗号化した暗号化データ及び当該暗号化キーデータを前記ディスク記憶媒体に記録する記録手段を有することを特徴とする請求項３記載のコピー防止システム。
【請求項５】　前記ディスク記憶媒体から記録されたデータを読出して、所定の出力形態に再生出力する再生手段を有し、
前記再生手段の再生出力時に、前記ディスク記憶媒体から前記暗号化キーデータ及び再生対象のコンテンツデータに対応する暗号化データを読出し、前記暗号化キーデータを使用して当該暗号化データを復号化する復号化手段を備えていることを特徴とする請求項３記載のコピー防止システム。
【請求項６】　前記識別データは装置固有の識別コードを示すと共に、前記ディスク記憶媒体に記録するデータの暗号化処理に必要な暗号データの記憶位置を示し、
前記ホストシステムは、前記制御手段により読出された識別データに基づいて前記暗号データを取得して、前記ディスク記憶媒体に記録するデータを暗号化するための暗号化キーデータを生成することを特徴とする請求項１又は請求項２記載のディスク記憶装置。
【請求項７】　前記識別データは装置固有の識別コードを示すと共に、前記ディスク記憶媒体に記録するデータの暗号化処理に必要な暗号データの記憶位置を示し、
前記暗号データ生成手段は、前記識別データを使用して前記暗号データを取得し、当該暗号データを使用して前記暗号化キーデータを生成することを特徴とする請求項３記載のコピー防止システム。
【請求項８】　前記ディスク記憶媒体に対するデータの記録を禁止するためのライトプロテクト手段を有することを特徴とする請求項１又は請求項２記載のディスク記憶装置、あるいは請求項３記載のコピー防止システム。
【請求項９】　ディスク記憶媒体をデータの記録媒体として使用するディスク記憶装置であって、
前記ディスク記憶媒体又は前記ディスク記憶媒体とは区別されたメモリ手段に記憶された装置固有の識別データを、ホストシステムからの特定コマンドに応じて読出す手段と、
前記読出し手段により読出した前記識別データを使用して、前記ディスク記憶媒体に記録するコンテンツデータを暗号化する暗号化機能を含むセキュリティ処理を実行するセキュリティ機能手段とを具備したことを特徴とするディスク記憶装置。

【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、例えば映像や音声などの情報コンテンツを記録するディスク記憶装置に関し、特に当該情報コンテンツのコピーを防止するための機能を有するディスク記憶装置または当該装置を利用したシステムに関する。
【０００２】
【従来の技術】近年、コンピュータデータだけでなく、映像や音声（特に音楽）などの情報コンテンツをディジタル化したデータ（コンテンツデータと表記する）を記憶する媒体として、高速アクセス及び大容量化が可能な小型のハードディスクドライブ（ＨＤＤ）が注目されている。ＨＤＤは、記憶媒体であるディスクとドライブ機構とが一体的に構成された構造が特徴である。特に小型のＨＤＤは、パーソナルコンピュータの内蔵型記憶装置だけでなく、ディジタルテレビやディジタルカメラ（ビデオカメラ及びスチールカメラ）などの記憶媒体として適用範囲が広がっていいる。
【０００３】ところで、コンテンツデータは、ディジタル放送、インターネット、または記録メディアなどを利用した配信や流通により、不特定多数のユーザに提供されることが一般的である。このため、コンテンツデータの取り扱いでは、著作権保護、端的にはコピー防止機能が重要である。
【０００４】

【発明が解決しようとする課題】前述したように、ディジタルのコンテンツデータは、インターネットやパーソナルコンピュータなどを利用して、コピーが容易である。このため、近年では、各種の記録メディア、コンピュータシステム、ネットワークなどの技術開発と関連して、コピー防止技術の開発が推進されている。しかしながら、コンテンツデータの記憶媒体としてＨＤＤを利用した装置やシステムでは、必ずしも適当で有効なコピー防止機能が開発されていない。

【０００５】そこで、本発明の目的は、有効なコピー防止機能を有し、結果的にコンテンツデータの著作権保護を実現できるディスク記憶装置及び同装置を利用したシステムを提供することにある。

【０００６】

【課題を解決するための手段】本発明の第１の観点は、通常のユーザデータの記録動作では、書き換え不可能なディスクの記録領域または内部メモリに、予め装置固有の識別データが記憶されたディスク記憶装置である。具体的には、識別データは、ディスク上でユーザデータの記録領域以外の冗長領域（代替セクタ）、または装置内部に設けられた制御情報を記憶するための不揮発性で書換え可能なＩＣメモリ（ＥＥＰＲＯＭ）に記憶される。更に、本装置は、パーソナルコンピュータなどのホストシステムから特定コマンドを受信すると、当該識別データを記録領域から読出して出力する機能を有する。

【０００７】このような構成であれば、ホストシステムは、映像や音声などのコンテンツデータをディスク記憶装置に記録する場合に、識別データを読出すことにより当該装置を識別できる。従って、ホストシステムは、コンテンツデータを記録したディスク記憶装置を管理できるため、結果的に当該コンテンツデータに対する無制限なコピーを防止する機能を実現できる。

【０００８】本発明の第２の観点は、前記のような装置固有の識別データを記憶したディスク記憶装置とホストシステムとを有するコピー防止システムである。本システムは、ディスク記憶装置に記憶された識別データを使用して、ディスク記憶媒体に記録するコンテンツデータを暗号化するための暗号化キーデータを生成する暗号データ生成手段を備えている。

【０００９】このような構成であれば、ディスク記憶装置毎にコンテンツデータを暗号化して記録することができるため、当該ディスク記憶装置を別のホストシステムがアクセスした場合に、記録したコンテンツデータの再生を防止することが可能となる。従って、結果的にディスク記憶装置に記録したコンテンツデータに対する無制限なコピーを防止する機能を実現できる。

【００１０】

【発明の実施の形態】以下図面を参照して、本発明の実施の形態を説明する。

【００１１】図１は同実施形態に関係するＨＤＤの要部を示すブロック図であり、図２は同実施形態に関係するコピー防止システムを説明するための概念図である。

【００１２】（ＨＤＤの構成）同実施形態のＨＤＤ１は、例えばカード型でホストシステム２に対して着脱可能なリムーバル（ｒｅｍｏｖａｌ）型の小型ディスクドライブを想定する。ＨＤＤ１は、カード型の筐体の内部に、記憶媒体であるディスク１０およびドライブ機構が一体的に設けられた構造である。ドライブ機構は主として、ディスク１０を回転させるスピンドルモータや、当該ディスク１０に対してデータのリード／ライト動作を実行するためのヘッドをシークさせるアクチュエータからなる（図示せず）。

【００１３】ＨＤＤ１は、ディスク１０及びドライブ機構以外に、データの記録再生及びデータ転送を処理するための制御・信号処理系を有する。制御・信号処理系は、データチャネル１１と、ディスクコントローラ（ＨＤＣ）１２と、バッファメモリ１３と、マイクロプロセッサ（ＣＰＵ）１４と、メモリ１５とを有する。データチャネル１１は、ヘッドによりディスク１０に記録すべきデータ信号及びディスク１０から読出されたデータ信号に対する各種の信号処理を実行する。ＨＤＣ１２は、ＨＤＤ１とホストシステム（同実施形態ではパーソナルコンピュータを想定する）２とのインターフェースを構成し、主としてデータ転送機能を有する。バッファメモリ１３は、ＨＤＣ１２により制御されて、ディスク１０から読出されたデータ（再生データ）及びホストシステム２から転送されたデータ（記録データ）を一時的に保存する。

【００１４】ＣＰＵ１４は、ＨＤＤ１のメイン制御装置であり、同実施形態のコピー防止機能に関係する制御動作を実行する。メモリ１５は、ＣＰＵ１４により制御されるＩＣメモリであり、通常では書き換え可能な不揮発性メモリ（例えばＥＥＰＲＯＭ）からなる。

【００１５】同実施形態のＨＤＤ１では、ディスク１０上の特定の記録領域に、ＩＤデータ１０Ａ及び暗号データ１０Ｂが予め記憶されている。特定の記録領域とは、通常のユーザデータ（後述するコンテンツデータやコンピュータデータ）の記録動作では書き換え不可能（アクセス不可）な代替セクタ（冗長記録領域）を想定する。ＩＤデータ１０Ａは、装置固有の識別コード及び暗号データ１０Ｂのアドレスを示す識別データである。また、暗号データ１０Ｂは、後述するように、ホストシステム２側でコンテンツデータの暗号化処理に必要な暗号化キーデータを生成するために使用するデータである。

【００１６】なお、ＩＤデータ１０Ａ及び暗号データ１０Ｂは、ＥＥＰＲＯＭ１５に記憶されていてもよい。ＣＰＵ１４は、ホストシステム２からＨＤＣ１２を介して、特定コマンドを受信すると、ディスク１０またはメモリ１５からＩＤデータ１０Ａ及び暗号データ１０Ｂを読出してホストシステム２に転送する。

【００１７】（コピー防止システム）同実施形態では、図２に示すように、映像や音声などの情報コンテンツをディジタル化したコンテンツデータを、サーバ３からインターネット４を介してパーソナルコンピュータ（ＰＣ）２に提供されるシステムを想定する。サーバ３は、コンテンツデータを暗号化キーデータ（共通キー）により暗号化し、当該暗号化データ３Ｂ及び当該暗号化キーデータを含むセキュリティ情報３Ａを送信する。

【００１８】ＰＣ２は、インターネット４から送信された暗号化データ３Ｂ及びセキュリティ情報３Ａをダウンロードし、後述するような手順により、内部に装着したＨＤＤ１にコピーする。なお、セキュリティ情報３Ａには、コピーを１回だけ許可するコピー制限情報も含まれている。

【００１９】このようなシステムにおいて、図１と図２と共に図４の乃フローチャートを参照して、ＨＤＤ１へのコピー動作（コンテンツデータの記録動作）を説明する。

【００２０】まず、ＰＣ２は、ＨＤＤ１に対して、ＩＤデータ１０Ａを読出すための特定コマンド（ＩＤデータ１０Ａのアドレスを含む）を発行する。ＣＰＵ１４は、特定コマンドの受信に応じて、ディスク１０の特定記録領域からＩＤデータ１０Ａを読出して、ＰＣ２に転送する（ステップＳ１）。なお、メモリ１５からＩＤデータ１０Ａを読出す場合も同様である。

【００２１】ＰＣ２は、受信したＩＤデータ１０Ａを使用して、ＨＤＤ１がセキュリティ機能が設けられている記憶媒体であることを認証する。更に、ＰＣ２はＩＤデータ１０Ａを使用して、暗号データ１０Ｂのアドレスを算出し、このアドレスを含む特定コマンドを発行する（ステップＳ２）。ＣＰＵ１４は、特定コマンドの受信に応じて、ディスク１０の特定記録領域から暗号データ１０Ｂを読出して、ＰＣ２に転送する（ステップＳ３）。

【００２２】ＰＣ２は、ＨＤＤ１固有の暗号データ１０Ｂを取得すると、当該暗号データ１０Ｂ及びダウンロードしたセキュリティ情報３Ａを使用して、暗号化キーデータ１０Ｃを生成する（ステップＳ４）。ＰＣ２は、生成した暗号化キーデータ１０ＣをＨＤＤ１に転送し、ディスク１０上の特定記録領域（代替セクタ）またはメモリ１５の指定領域に記録する（ステップＳ５）。この場合、暗号化キーデータ１０Ｃの記録アドレスは、ＨＤＤ１固有の暗号データ１０Ｂに基づいて設定される。

【００２３】次に、ＰＣ２は、生成した暗号化キーデータ１０Ｃを使用して、ダウンロードしたコンテンツデータ（共通キーによる暗号化データ）３Ｂを暗号化して、ＨＤＤ１に転送する（ステップＳ６）。ＨＤＤ１は、通常のユーザデータと同様に、暗号化したコンテンツデータ１０Ｄをディスク１０上の記録領域に記録する（ステップＳ７）。

【００２４】以上の処理により、ＰＣ２は、サーバ３から取得したコンテンツデータを暗号化して、ＨＤＤ１にコピーする。ＰＣ２は、サーバ３からのセキュリティ情報３Ａにに基づいて、１回目のコピーが終了後に２回目以降のコピーを禁止するためのロック処理を実行する。

【００２５】（再生システム）次に、図３及び図５のフローチャートを参照して、同実施形態の再生システムを説明する。

【００２６】前述したように、ＰＣ２により、ＨＤＤ１には暗号化されたコンテンツデータ１０Ｄが記録されている。ここで、ＰＣ２からＨＤＤ１を取出して、図３に示すように、再生プレーヤ５に接続するシステムを想定する。再生プレーヤ５は、ＨＤＤ１から読出したコンテンツデータから、映像信号や音声信号を再生して例えばディジタルテレビなどの再生出力装置５１に出力する。

【００２７】再生プレーヤ５は、ＨＤＤ１が接続されて再生動作が開始されると、ＨＤＤ１からＩＤデータ１０Ａを読出す（ステップＳ１０）。ここで、再生プレーヤ５のＣＰＵが、前述のＰＣ２と同様に、特定コマンド（ＩＤデータ１０Ａのアドレスを含む）を発行して、ディスク１０の特定記録領域からＩＤデータ１０Ａを読出す。このＩＤデータ１０Ａを使用して、再生プレーヤ５のＣＰＵは、ＨＤＤ１がセキュリティ機能が設けられている記憶媒体であることを認証する。

【００２８】さらに、再生プレーヤ５は、受信したＩＤデータ１０Ａを使用して、暗号データ１０Ｂのアドレスを算出し、ＨＤＤ１から当該暗号データ１０Ｂを読出す（ステップＳ１１，Ｓ１２）。再生プレーヤ５は、取得した暗号データ１０Ｂに基づいて、暗号化キーデータ１０Ｃのアドレスを算出し、ＨＤＤ１から当該暗号化キーデータ１０Ｃを読出す（ステップＳ１３，Ｓ１４）。

【００２９】再生プレーヤ５は、内蔵している復号化処理部（専用回路またはＣＰＵの機能）５０により、読出した暗号化キーデータ１０Ｃを使用して、ＨＤＤ１に記録されているコンテンツデータ（暗号化データ）１０Ｄを復号化して、元のコンテンツデータに再生する（ステップＳ１５，Ｓ１６）。再生出力装置５１は、再生された映像をディスプレイ上に表示出力し、スピーカから再生された音声を出力する。

【００３０】以上のように同実施形態のシステムであれば、ＨＤＤ１の固有のＩＤデータ及び暗号データを利用して暗号化したコンテンツデータを、ＨＤＤ１に記録することになる。従って、仮にＨＤＤ１を別のＨＤＤや記録メディアにコピーする場合に、当該ＨＤＤ１に対応するＰＣ２や、セキュリティ機能が設けられた特別の再生プレーヤ５は、ＨＤＤ１から固有のＩＤデータを認証しないと、暗号データを読出すことはできないため、コピーをしても再生できない。これにより、ＨＤＤ１に記録したコンテンツデータを、他のＨＤＤや記録メディアでは再生することを防止できるため、結果的に当該コンテ

ンツデータの著作権の保護を実現することが可能となる。

【００３１】なお、同実施形態では、インターネットから予め暗号化されたコンテンツデータ（著作権が保護されたデータ）を、ＨＤＤ１にダウンロードする場合を想定したが、これに限らず、ディジタル放送や他の記録メディアからコピーされた場合でも適用できる。

【００３２】（変形例１）図６は、同実施形態の変形例を示すブロック図である。即ち、本変形例は、前述した同実施形態のコピー防止機能を、ＣＰＵではなく、専用のセキュリティ・チップ（メモリを内蔵したＩＣ）６１を内蔵したＨＤＤ６０である。

【００３３】本ＨＤＤ６０では、セキュリティ・チップ６１は予めＩＤデータ１０Ａ及び暗号データ１０Ｂを記憶し、ＨＤＣ６２を介して入力されたホストシステム２からの特定コマンドに応じて当該ＩＤデータ１０Ａ及び暗号データ１０Ｂをホストシステム２に転送する機能を備えている。なお、コピー防止機能の動作は、前述の同実施形態の場合と同様であるため、説明を省略する。

【００３４】このような本変形例の方式であれば、ＨＤＤのＣＰＵの負担を軽減し、ディスク１０上の特定記録領域に対するアクセスを不要にできる。また、セキュリティ・チップ６１には、同実施形態に関係するコピー防止機能以外のセキュリティ機能を含ませることも容易である。具体的には、例えばコンテンツを供給するサーバと連動して、１週間毎に暗号データを変更するなどの機能である。また、ＩＤデータ１０Ａ及び暗号データ１０Ｂを、セキュリティ・チップ６１及びディスク１０の双方に記憶させることにより、セキュリティ機能の効果を高めることが可能となる。

【００３５】（変形例２）図７及び図８は、同実施形態のＨＤＤ１において、いわゆるライトプロテクト機能を有する変形例に関する。

【００３６】即ち、本変形例のＨＤＤ７０は、図７に示すように、カード型筐体（例えばＰＣＭＣＩＡ規格）の中にディスク、ドライブ機構及び制御・信号処理系を内蔵しており、その外側にライトプロテクト用スイッチ（例えばスライドスイッチ）７１を有する。また、筐体の外側には、通常ではパーソナルコンピュータなどのホストシステムに接続するためのコネクタが設けられている。さらに、図８を参照して、ライトプロテクト機能を説明する。

【００３７】ライトプロテクト用スイッチ７１がオン（即ち、ライトプロテクト機能の有効を意味する）されると、ＨＤＤ７０の内部に設けられたラッチ回路７３がその情報（ライトプロテクト）をラッチする。ホストシステム２は、コネクタ７２によりＨＤＤ７０に接続すると、ライトプロテクト機能のオン／オフを確認するためのコマンドを発行する。

【００３８】ＨＤＤ７０では、内部ロジック（ＨＤＣ及びＣＰＵの各機能）７４がホストシステム２からのコマンドに応じて、ラッチ回路７３のクロック入力にクロックパルスを供給して、当該ラッチ回路７３から情報を読出す。そして、内部ロジック（ＨＤＣ及びＣＰＵの各機能）７４は、読出した情報をコネクタ７２を介してホストシステム２に出力する。ホストシステム２は、受信した情報に基づいて、ライトプロテクト機能が有効であるか否かを識別する。

【００３９】以上のようなライトプロテクト機能を有するＨＤＤであれば、ユーザがスイッチ７１を操作するだけで、ＨＤＤのディスクに対するデータの書込み動作を禁止できる。従って、特にカード型などの着脱可能なＨＤＤにおいて、記録したデータを保存したい場合に、ライトプロテクト機能を有効にすれば、保存データを確実に保護することが可能となる。これにより、当該ＨＤＤを、従来の映像や音声を保存する記録メディアとして使用することが可能となる。

【００４０】なお、同実施形態及び各変形例は、ディスク記憶装置としてＨＤＤを想定したが、他のディスク記憶媒体である書込み可能な光ディスク装置や光磁気ディスク装置にも適用することが可能である。

【００４１】

【発明の効果】以上詳述したように本発明によれば、第１にディスク記憶媒体に記録するコンテンツデータの無制限なコピーを確実に防止する機能を備えたディスク記憶装置及び同装置を適用したシステムを提供することができる。従って、特にディスク記憶装置として着脱可能な小型の装置に適用すれば、有効なコピー防止機能により、結果的にコンテンツデータの著作権保護を実現することができる。第２に、ライトプロテクト機能を有するディスク記憶装置を実現することにより、保存データを確実に保護できる。従って、特に着脱可能な小型のディスク記憶装置に適用すれば、コンテンツデータを保存するための記録メディアとして使用することが可能となる。

【図面の簡単な説明】

【図１】本発明の実施形態に関係するＨＤＤの要部を示すブロック図。

【図２】同実施形態に関係するコピー防止システムを説明するための概念図。

【図３】同実施形態に関係するデータ再生系を説明するための概念図。

【図４】同実施形態に関係するデータ記録動作を説明するためのフローチャート。

【図５】同実施形態に関係するデータ再生動作を説明するためのフローチャート。

【図６】同実施形態の変形例１に関係するＨＤＤの要部を示すブロック図。

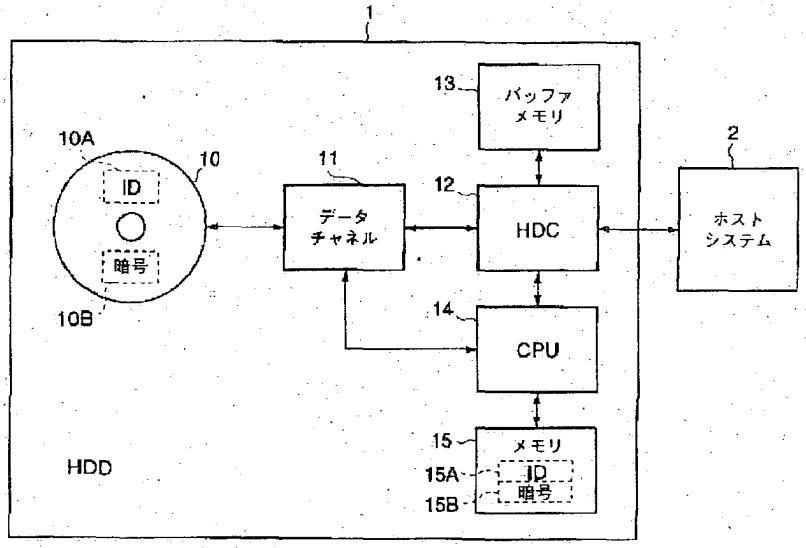
【図７】同実施形態の変形例２に関係するＨＤＤの外観を説明するための図。

【図８】同変形例２に関係するＨＤＤの内部構成を説明するための図。

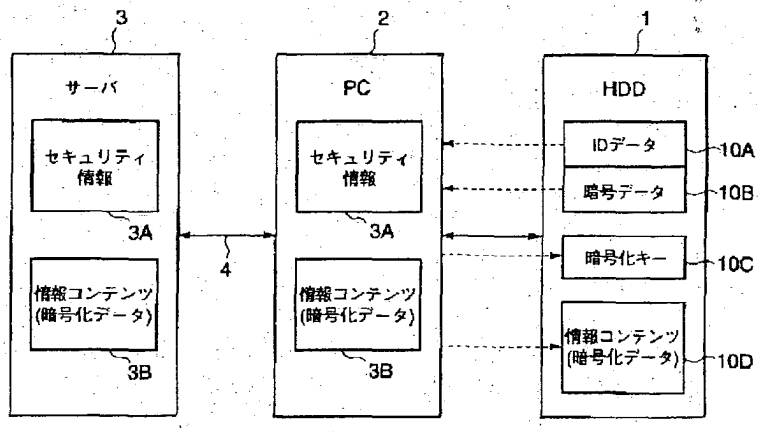
【符号の説明】

１…ディスク記憶装置（ＨＤＤ）
２…ホストシステム（パーソナルコンピュータ）
３…サーバ
４…インターネット
５…再生プレーヤ
１０…ディスク
１１…データチャネル
１２…ディスクコントローラ（ＨＤＣ）
１３…バッファメモリ
１４…マイクロプロセッサ（ＣＰＵ）
１５…メモリ（ＥＥＰＲＯＭ）
５０…復号化処理部
５１…再生出力装置
６１…セキュリティ・チップ
７１…ライトプロテクトスイッチ

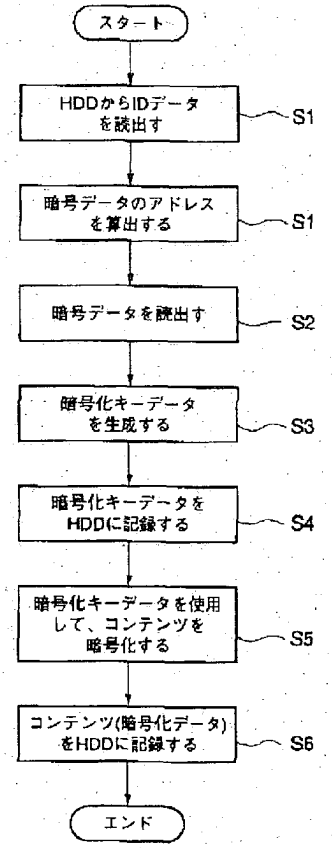
【図１】



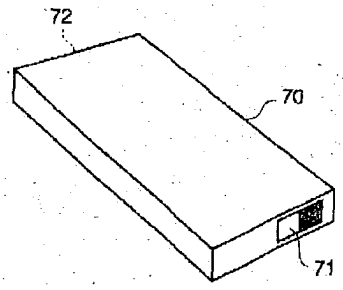
【図２】



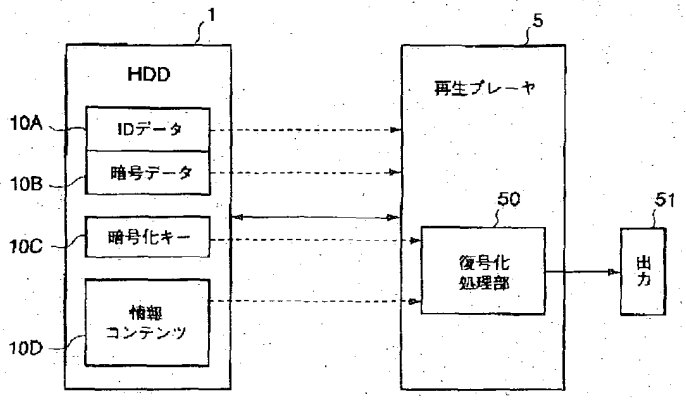
【図４】



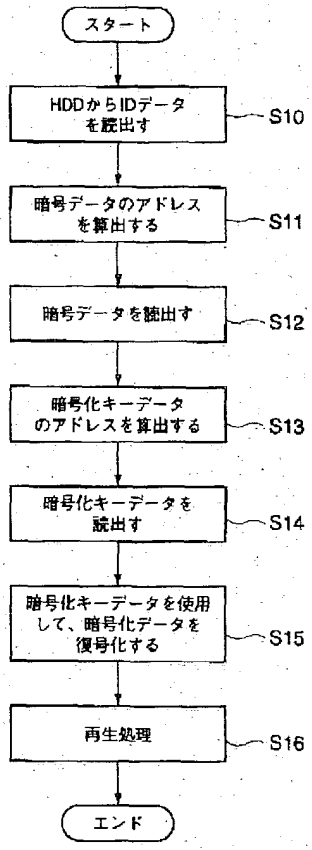
【図７】



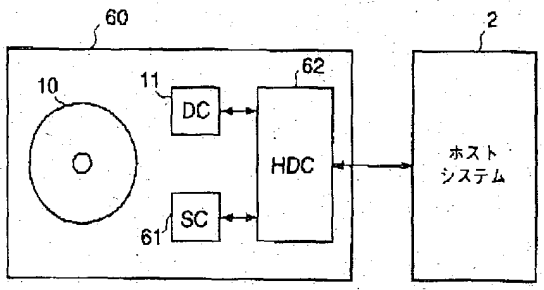
【図３】



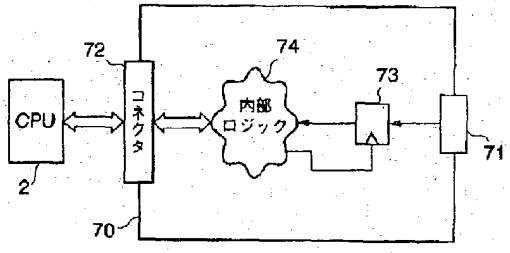
【図５】



【図６】



【図８】



フロントページの続き

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
Ｇ１１Ｂ　19/02	５０１	Ｇ１１Ｂ　19/02	５０１Ｑ	
19/12	５０１	19/12	５０１Ｋ	

(72)発明者　粟津　浩一
東京都港区芝浦一丁目１番１号　株式会社
東芝本社事務所内

Ｆターム(参考) 5B017 AA02 AA06 BA05 BA07 CA07
CA12 CA14 CA16
5B065 BA01 CA11 PA02 PA04 PA16
5D044 BC01 CC04 DE49 DE50 FG10
FG18 GK17 HL01 HL08 HL11
5D066 EA02 EA13 EA17 EA21 EA22
HA01